Virtual Attacks – physical damages

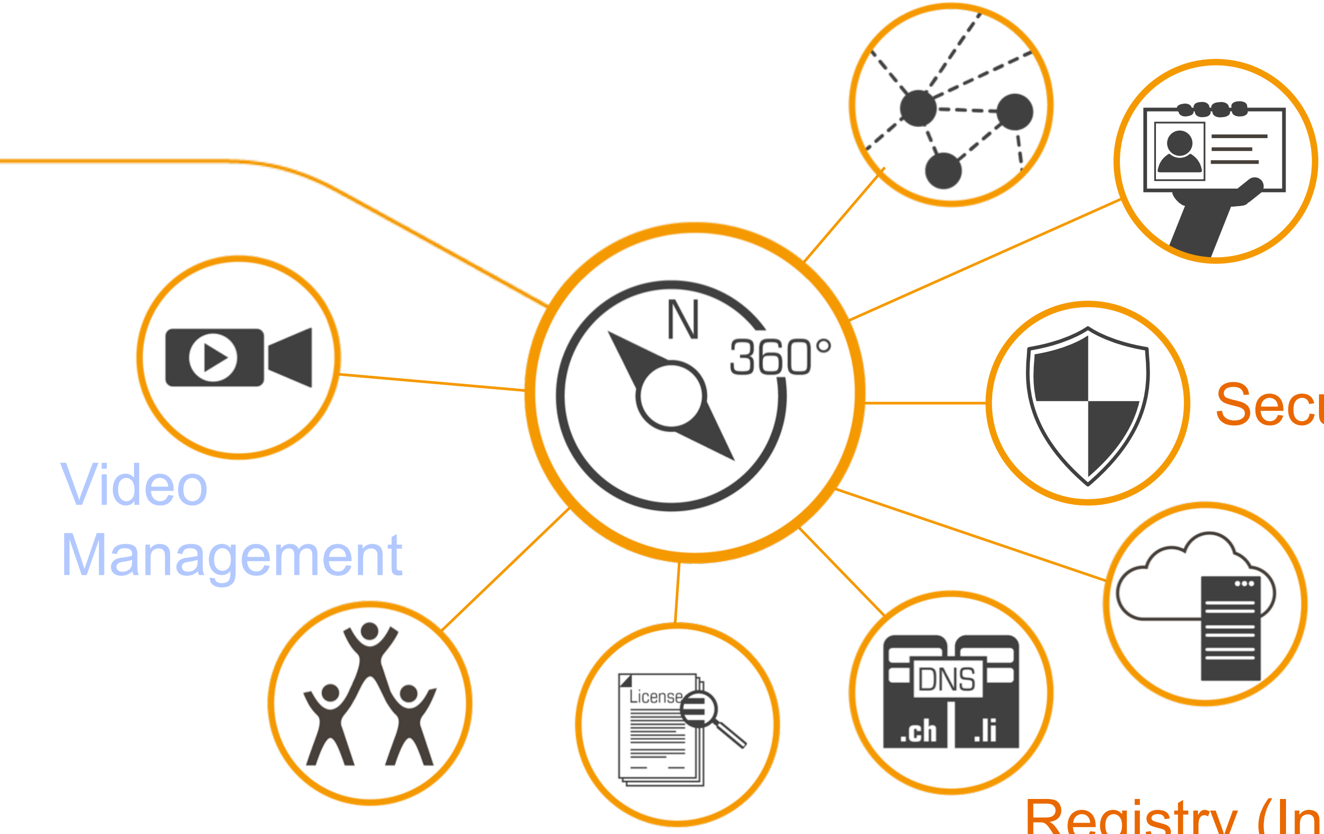
Everything goes digital – what about security?

SWITCH

Martin Leuthold
martin.leuthold@switch.ch

Brugg-Windisch, March 6, 2018

SWITCH – Swiss internet pioneer



Network (Swiss NREN)

Trust & Identity

Security (SWITCH-CERT)

Infrastructure & Data Services

Registry (Internet early adopters)

Procurement

Collaboration

Video Management

Gartner 2017: Estimated growth of installed IoT devices

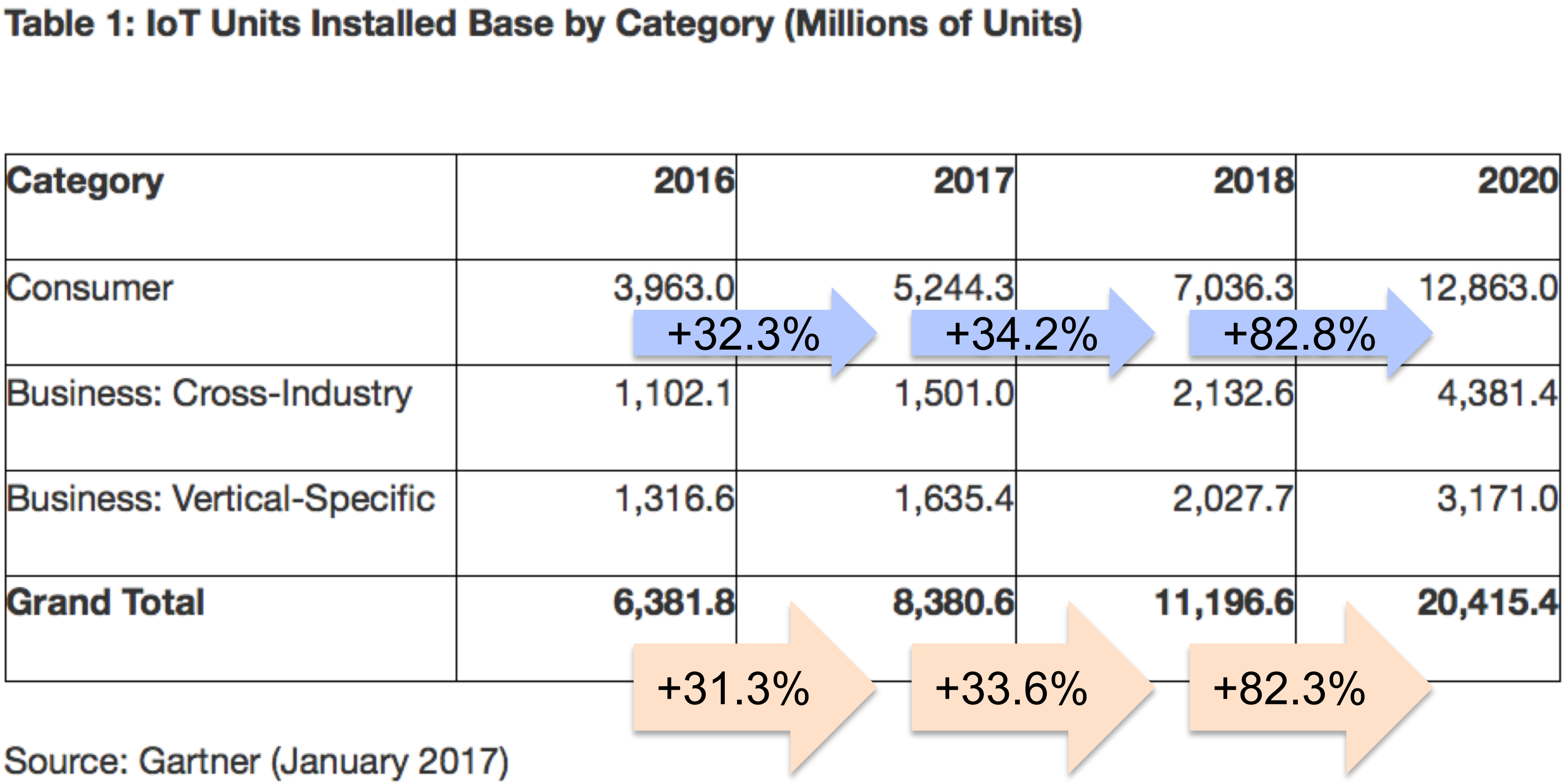


Table 1: IoT Units Installed Base by Category (Millions of Units)

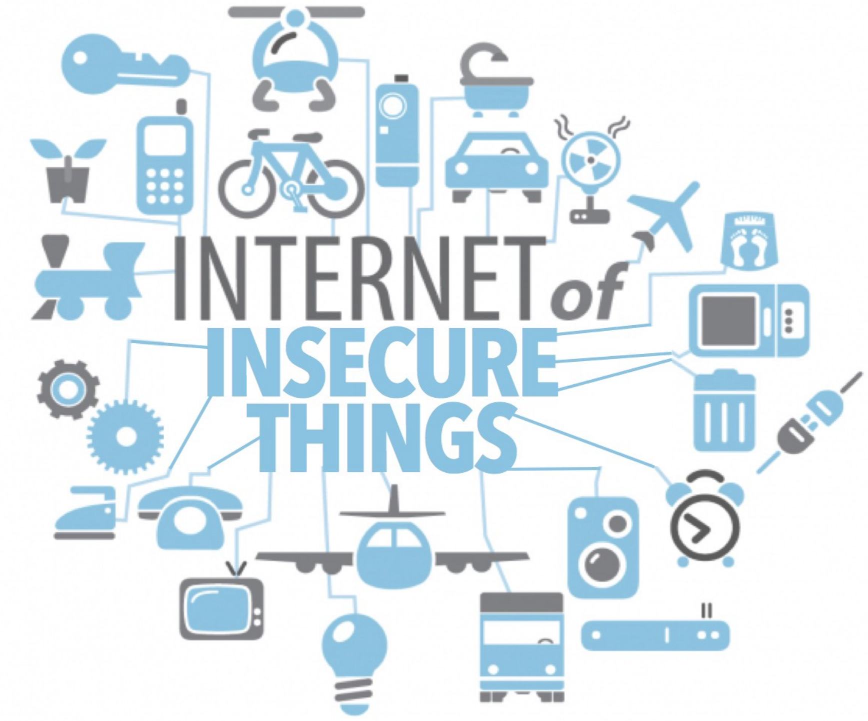
Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	**6,381.8**	**8,380.6**	**11,196.6**	**20,415.4**

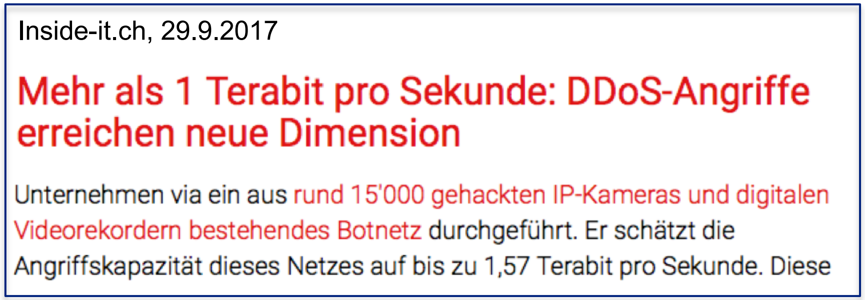
Source: Gartner (January 2017)

+32.3% +34.2% +82.8%

+31.3% +33.6% +82.3%

Market failure results in “Consumer Internet of Insecure Things”




Inside-it.ch, 29.9.2017

Mehr als 1 Terabit pro Sekunde: DDoS-Angriffe erreichen neue Dimension

Unternehmen via ein aus rund 15'000 gehackten IP-Kameras und digitalen Videorekordern bestehendes Botnetz durchgeführt. Er schätzt die Angriffskapazität dieses Netzes auf bis zu 1,57 Terabit pro Sekunde. Diese

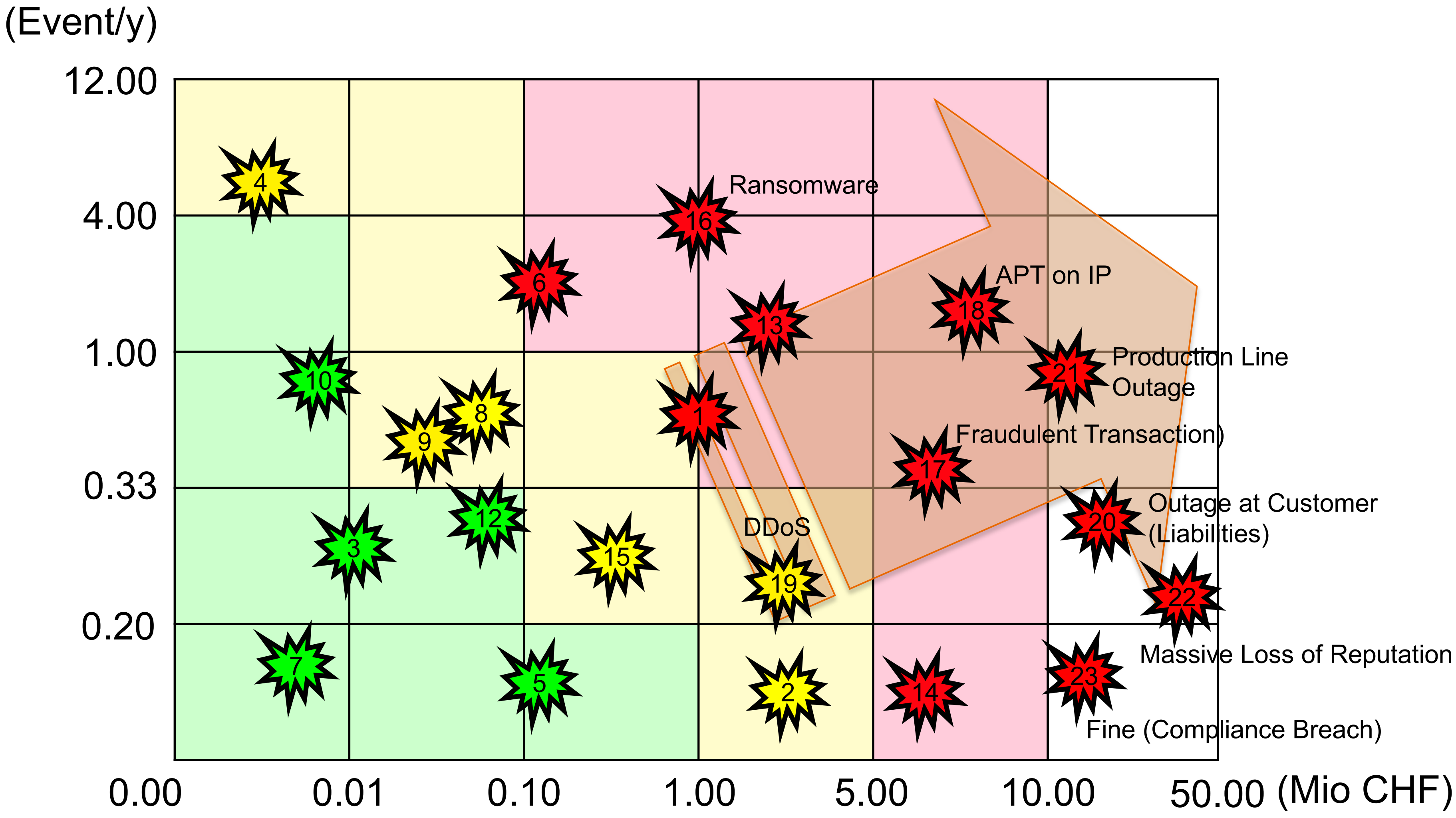
Regulation needed – minimum ICT-security standards for CIoT, e.g. no standard passwords and automatic patching functionality.

What about your efforts to secure your digitalization efforts – e.g. smart building technology, internet channels? Are your IP cams secure?

But why should you be interested in security …?

Source https://medium.com/enrique-dans/the-internet-of-insecure-things-f0a3a47aa7f7

Risk landscape changers: Cybercrime & digitalization (attack surface & business impact)



Smart Home Honeypot – Project “Haunted House” (by Koramis, supported by Sophos, November 2017)

Testphase “Secured” (6 weeks)

- Recommended configurations of the vendors
- Changed and secure passwords on all devices
- Average 1’500 attacks per day
- Most attacks originated form China, US, Mexico, India, Brazil & Russia
- 4 ”brute force” attacks on devices (not successful)

Testphase “Standard” (3 weeks)

- Standard passwords not changed
- Average 3’800 attacks per day
- 27 ”brute force” attacks, most of them automated

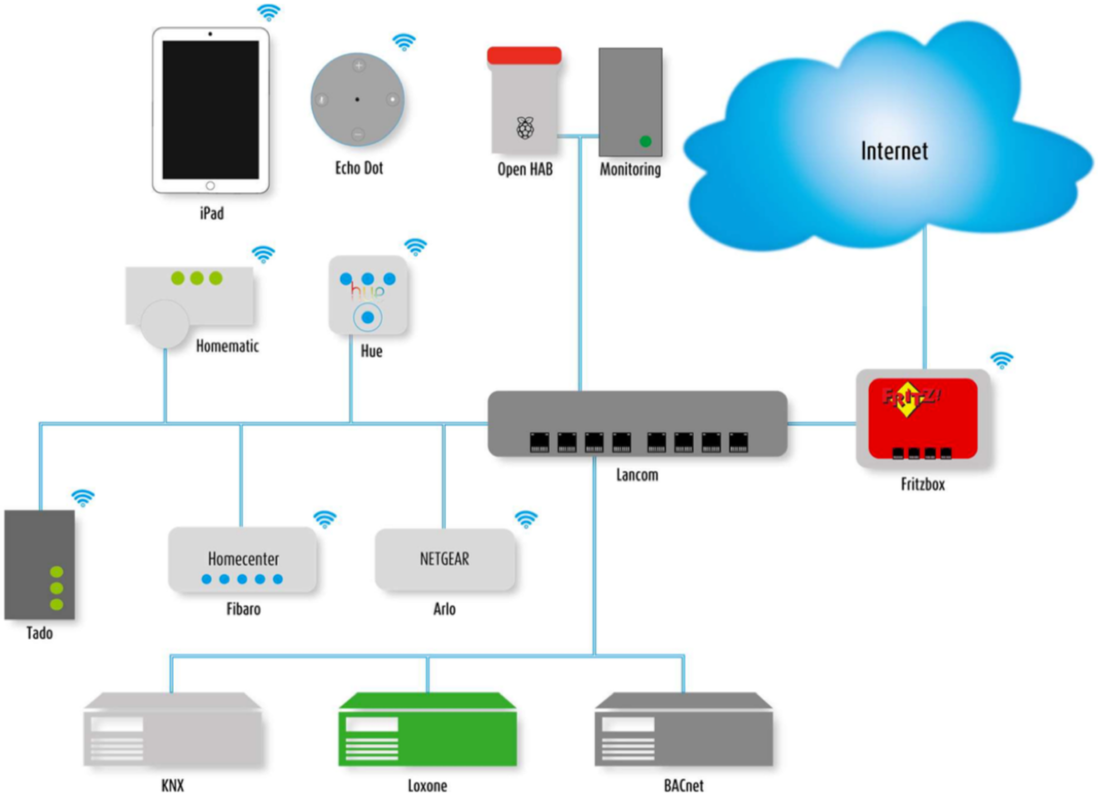
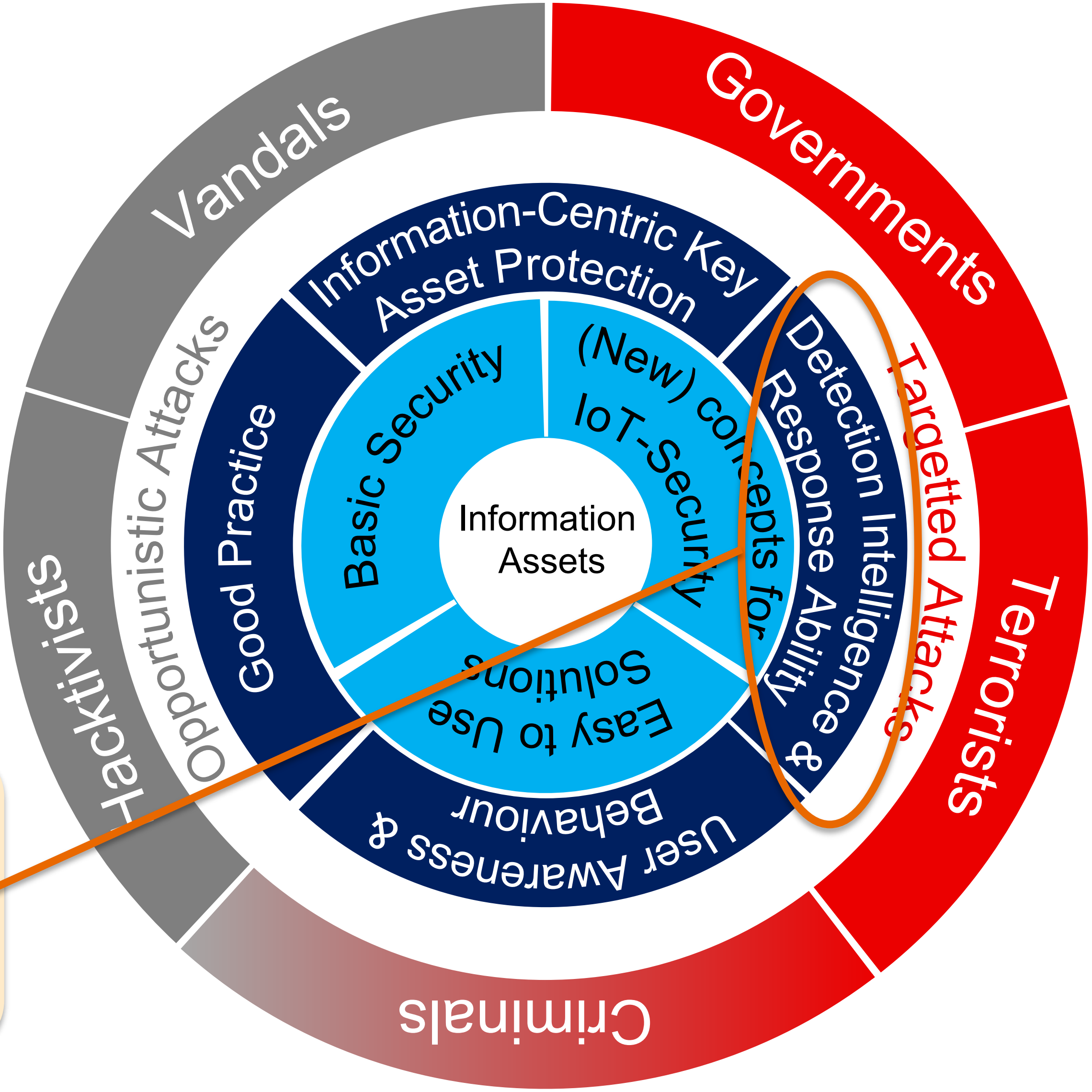


Abbildung 2.3: Layout Haunted House

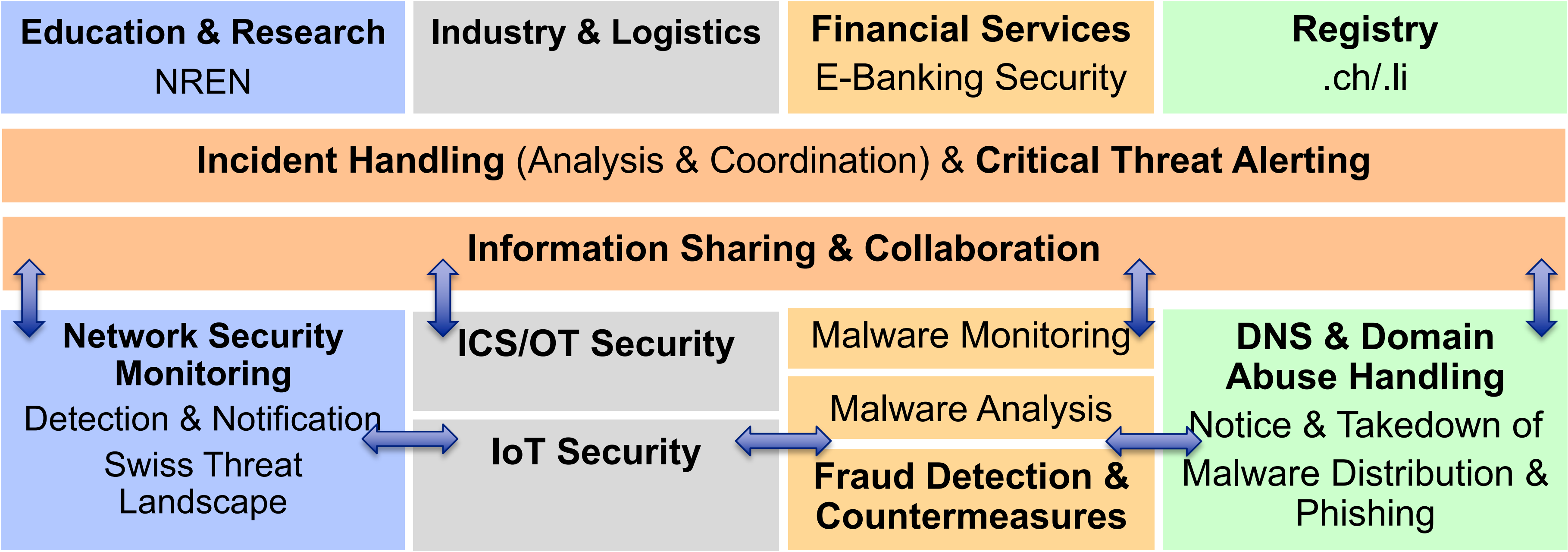
Baseline security still needed, new topics added, limited resources

- Critical attacker categories: organized cybercrime & governments
- Current key topics:
  - Baseline security operations on industry good practice level
  - Continuing awareness programs
- Upcoming key topics:
  - Information-centric protection of business-critical information
  - Avoid shadow IT: balance of usability, cost, functionality, efficient operations & security
  - New concepts for IoT security
  - Fast detection of attacks and immediate reaction.
  - Regionally relevant, high quality threat intelligence.
- Cooperation: leverage competence centers



Source: Roger Halbheer (adapted).

Leveraging synergies in a competence center – reduce exposure time & improve quality



Education & Research
NREN

Industry & Logistics

Financial Services
E-Banking Security

Registry
.ch/.li

Incident Handling (Analysis & Coordination) & **Critical Threat Alerting**

Information Sharing & Collaboration

Network Security Monitoring
Detection & Notification
Swiss Threat Landscape

ICS/OT Security

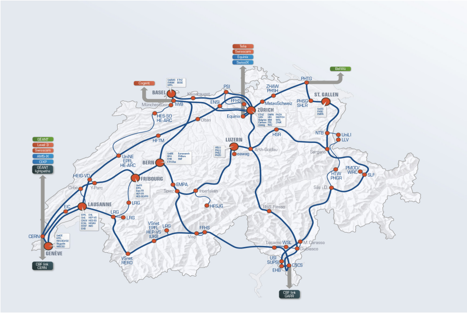
IoT Security

Malware Monitoring

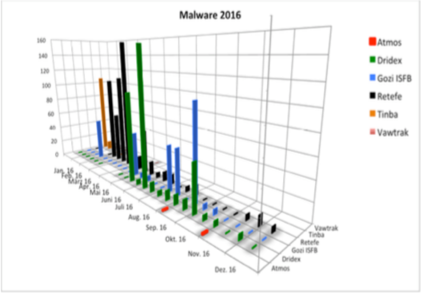
Malware Analysis

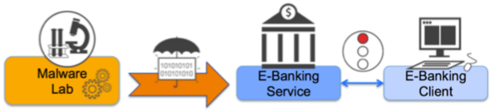
Fraud Detection & Countermeasures

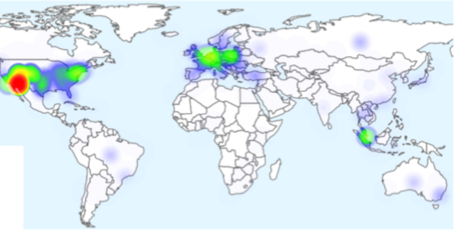
DNS & Domain Abuse Handling
Notice & Takedown of Malware Distribution & Phishing



Source: enisa



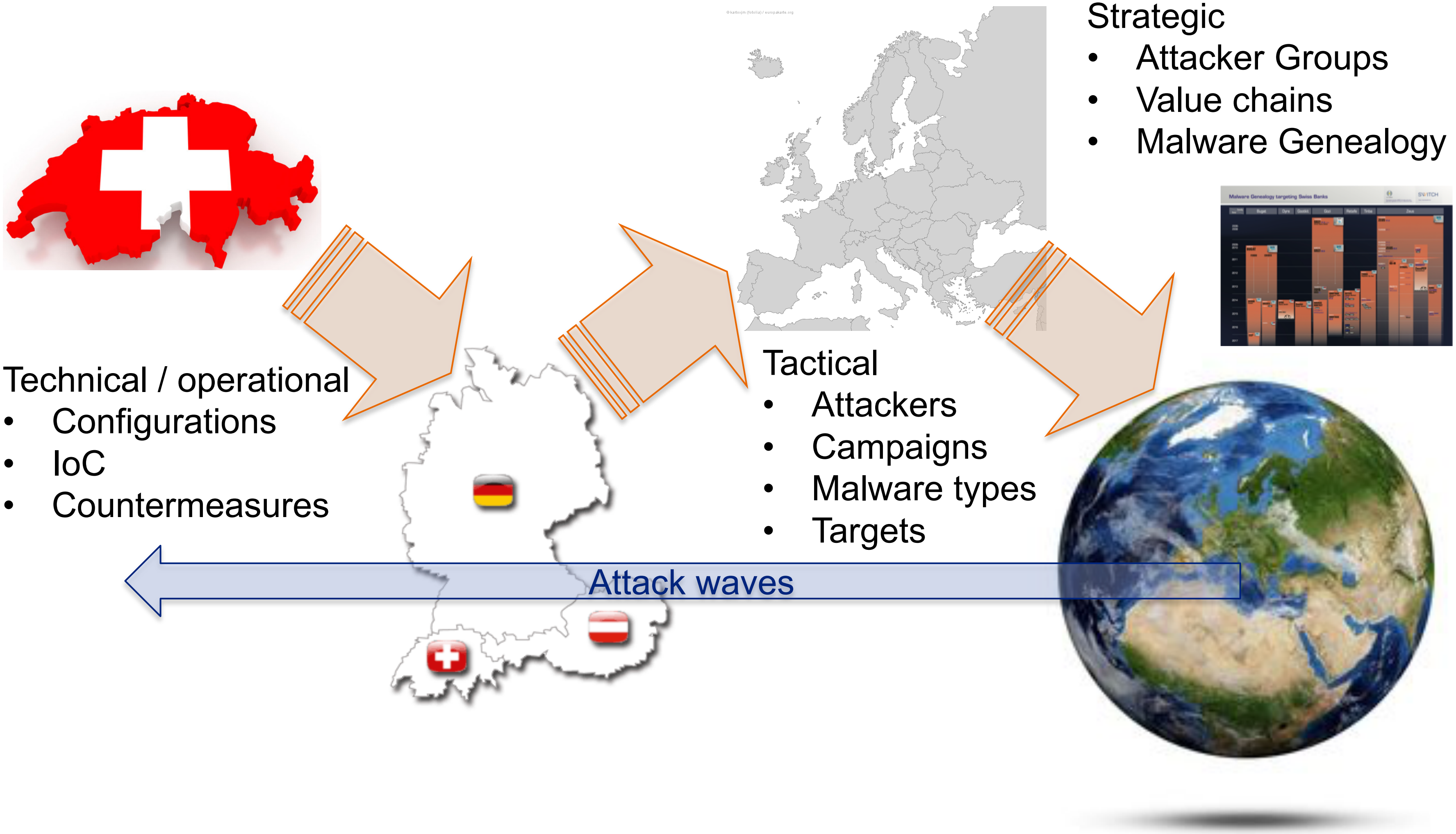




Distribution of web servers, which are misused by the Angler exploit-kit.

Swiss focus – worldwide operational cooperation

SWITCH



Strategic
- Attacker Groups
- Value chains
- Malware Genealogy

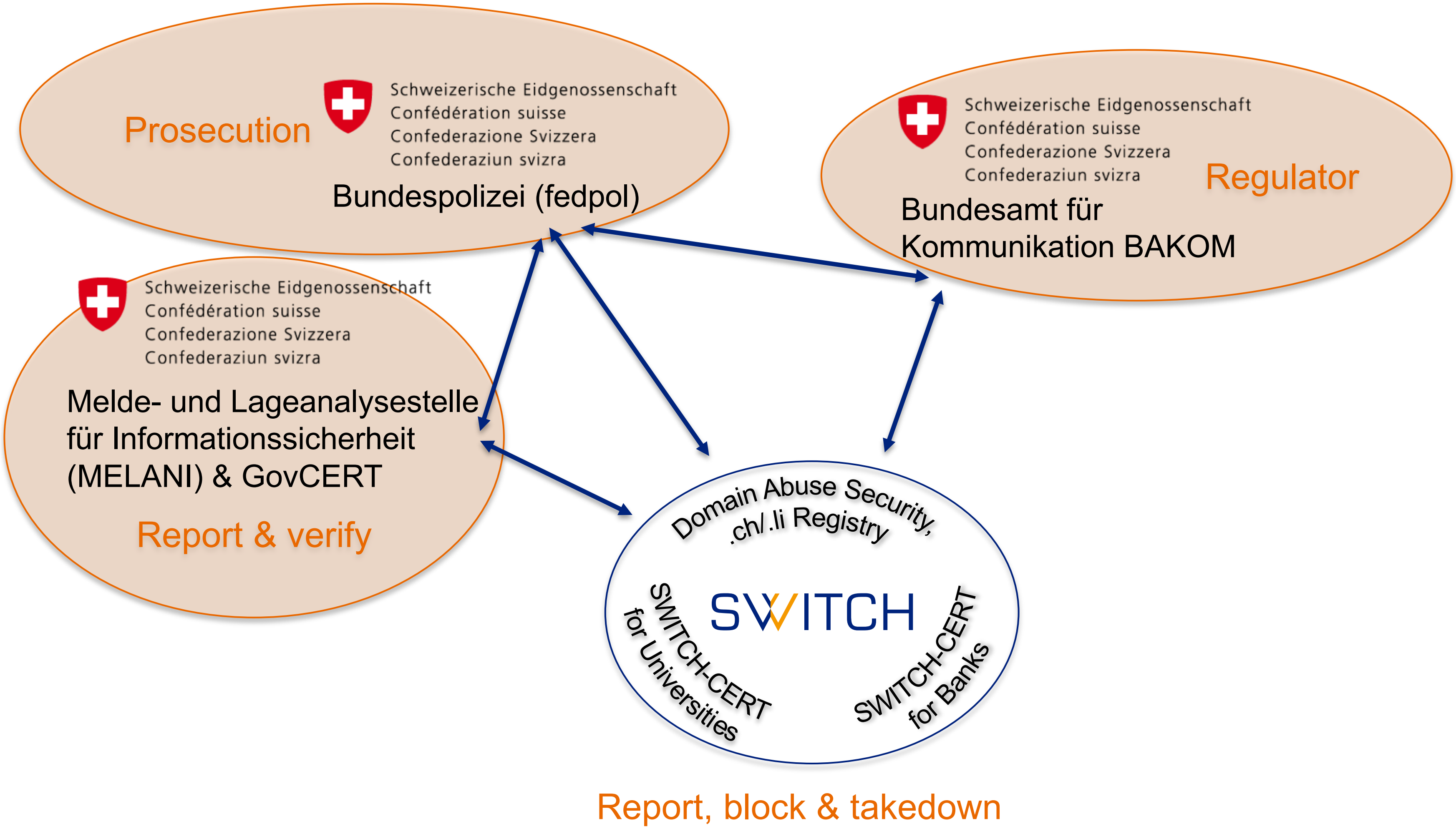
Tactical
- Attackers
- Campaigns
- Malware types
- Targets

Technical / operational
- Configurations
- IoC
- Countermeasures

Sources (pictures): www.sfdrs.ch, www.newstroll.de, www.bgu.tum.de

Worldwide leading Swiss domain abuse process – the power of collaboration!

SWITCH



Prosecution

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundespolizei (fedpol)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Regulator

Bundesamt für Kommunikation BAKOM

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Melde- und Lageanalysestelle für Informationssicherheit (MELANI) & GovCERT

Report & verify

Domain Abuse Security, .ch/.li Registry

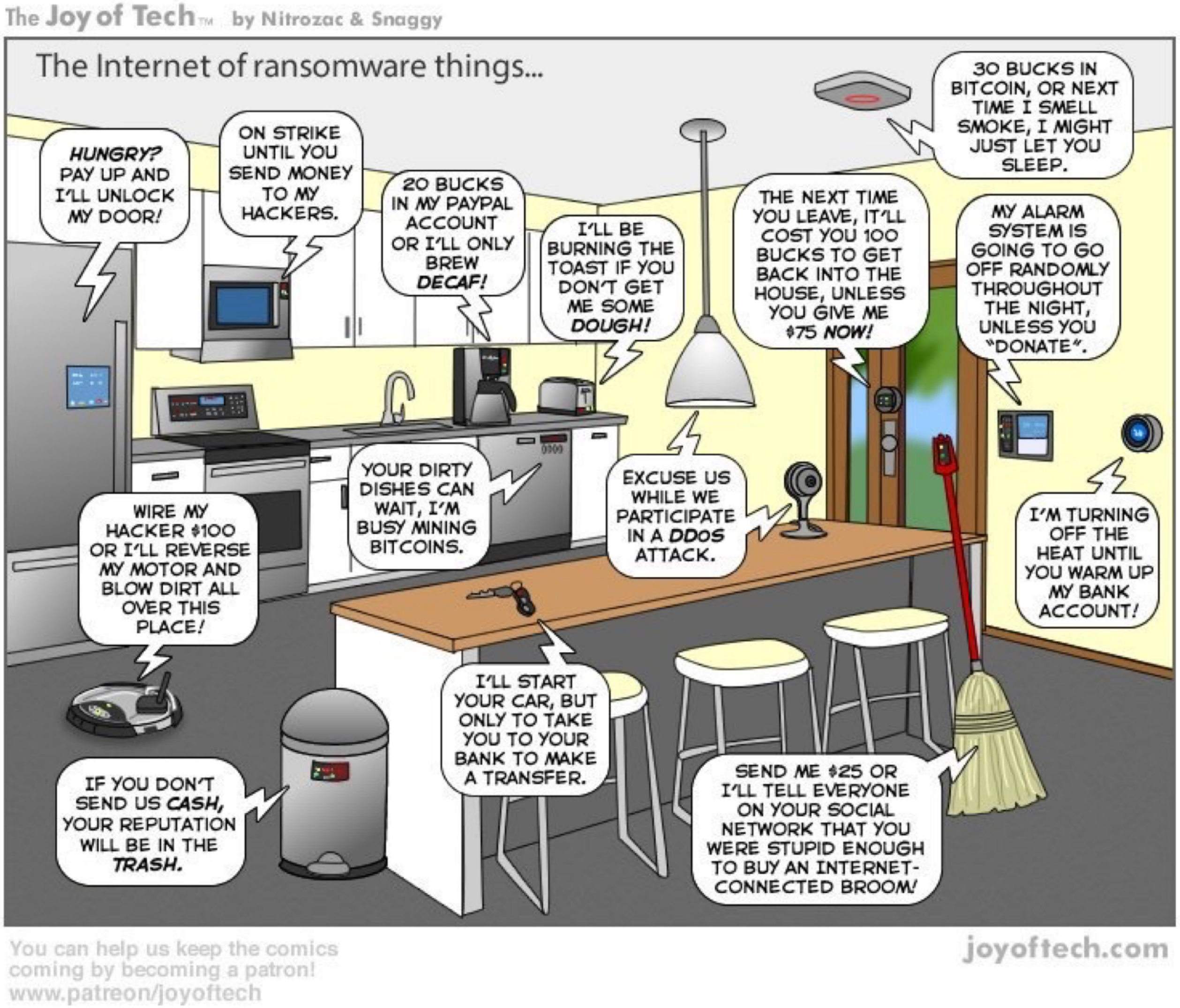
SWITCH

SWITCH-CERT for Universities

SWITCH-CERT for Banks

Report, block & takedown

Security by design is by far less effort than incident & crisis management!


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

Digitalization is based on trust - treat security as business enabler and not as a minor pain to be handled by the IT department.

Manage the ICT-security aspects of your digitalization efforts proactively.

Include ICT-security in all design & implementation stages.

Questions?

SWITCH

Working for a better digital world

Website:	http://www.switch.ch/security
Blog:	http://securityblog.switch.ch
Twitter:	@switchcert